УДК 342.9:004.7(477)

А. В. Форос
профессор кафедры кибербезопасности
и информационного обеспечения
Одесского государственного университета внутренних дел,
кандидат юридических наук, доцент (Украина)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ОБЪЕКТ ИНФОРМАЦИОННОГО ПРАВА

Процессы формирования информационного общества оказывают воздействие на многие элементы государственности, затрагивают как национальные, так и международные системы социальных регуляторов отношений государств, народов, юридических и физических лиц. За последнее время в Украине осуществился переход от информационной закрытости к общепринятым в мировой практике методам регулирования информационных отношений, формированию новой правовой отрасли – информационной. Именно сложность регулирования общественных отношений, складывающихся в информационной сфере, привела в ряде стран к выделению информационного права в самостоятельную отрасль. Провозглашение политического и идеологического плюрализма, свободы массовой информации, отмены цензуры привели к многократному увеличению объема информации. Поток информации, который практически не поддается контролю, создает благоприятную почву для нарушения прав личности. Законотворческая деятельность привела к созданию множества нормативных актов, каждый из которых содержит нормы о правах, свободах и обязанностях личности.

В контексте государственной информационной политики речь должна идти не только о правах граждан, юридических лиц и государства на свободное получение, распространение и использование информации, но и о необходимости защиты и рациональном использовании государственных информационных ресурсов, защите конфиденциальной информации и интеллектуальной собственности.

Информационная безопасность является важной самостоятельной сферой, а также неотъемлемой частью других сфер обеспечения национальной безопасности. Эксперты отмечают ухудшение ситуации в мире, рост нестабильности, конфликтного потенциала и военной опасности. Усиление напряженности происходит на фоне развертывания глобального экономического кризиса.

Информационная безопасность подчеркивает важность информации в современном обществе – понимание того, что информация – это ценный ресурс, основной материальный продукт.

В научной литературе принято рассматривать информационную безопасность как состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внешних и внутренних угроз. Согласно действующему законодательству информационная безопасность является составляющей национальной безопасности.

Для национальной безопасности наиболее актуальными являются риски и угрозы внутренние, а именно:

– неспособность правящих кругов сформировать и реализовать согласованную стратегию развития страны;

– сращение власти и бизнеса, высокий уровень коррупции;

– внутренняя политическая нестабильность и некомпетентность власти;

– существенные региональные различия в политико-идеологических и внешнеполитических ориентациях населения, что создает предпосылки для раскола общества;

– снижение уровня доходов населения и рост социального недовольства как следствие углубления экономического кризиса;

– угроза установления авторитарного режима.

Средние экспертные оценки свидетельствуют, что среди внутренних угроз, наибольшую (именно «высокую») степень угрозы для национальной безопасности создают отсутствие консолидации общества и его элиты, а также низкая эффективность государственного управления.

Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода.

Цели информационной безопасности – обезопасить ценности системы, защитить и гарантировать соблюдение качественных характеристик информации и минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена. Информационная безопасность требует учета всех событий, в ходе которых информация создается, модифицируется, к ней обеспечивается доступ или она распространяется.

Согласно Стратегии национальной безопасности Украины к угрозам информационной безопасности следует отнести: ведение информационной войны против Украины; отсутствие целостной коммуникативной политики государства; недостаточный уровень медиакультуры общества. Помимо этого установлены Приоритеты обеспечения информационной безопасности: обеспечение наступательности мер политики информационной безопасности на основе ассиметричных действий, направленных против всех форм и проявлений информационной агрессии; создание интегрированной системы оценки информационных угроз и оперативного реагирования на них; противодействие информационным операциям против Украины, манипуляциям с общественным сознанием и распространению искаженной информации; защита национальных ценно-

стей и укрепление единства украинского общества; разработка и реализация скоординированной информационной политики органов государственной власти; выявление субъектов украинского информационного пространства, созданных или используемых Россией для ведения информационной войны против Украины; усовершенствование профессиональной подготовки в сфере информационной безопасности.

Таким образом, информационная безопасность это состояние защищенности информационного пространства, обеспечивающее формирование и развитие этого пространства в интересах личности, общества и государства. Информационная безопасность дает гарантию того, что достигаются следующие цели: конфиденциальность информации; целостность информации и связанных с ней процессов (создания, ввода, обработки и вывода); доступность информации, когда она необходима; учет всех информационных процессов.

На наш взгляд, формирование режима информационной безопасности – проблема комплексная. Меры по ее решению условно можно подразделить на такие уровни:

законодательный или правовой (законы, нормативные акты, стандарты и т. п.);

административный (действия общего характера, предпринимаемые руководством организации для обеспечения информационной безопасности);

морально-этический (различные нормы поведения, несоблюдение которых ведет к падению престижа определенного человека или целой организации);

физический (механические, электро- и электронно-механические препятствия на возможных путях проникновения потенциальных нарушителей);

криптографический (использование методов шифрования и кодирования информации);

аппаратно-программный (электронные устройства и специальные программы защиты информации).

Единая совокупность всех этих мер, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образует систему защиты. Определяющим фактором в проблематике теории организации информационной безопасности является выяснение всех ее направлений на основе комплексного подхода к изучению методов защиты.